ABSTRACT OF THE DISCLOSURE

The Stickelberger element computing device computes a Stickelberger element ω in an ab cyclotomic; the Jacobian addition candidate value computing device computes the Jacobian addition candidate value j and a prime number p corresponding to the Jacobian addition candidate value j, based on the prime number a, the prime number b, the size n of an encryption key, and the Stickelberger element ω; the order candidate value computing device computes a class H consisting of a plurality of candidate values for the order of the Jacobian group of an algebraic curve, based on the prime number a, the prime number b, and the Jacobian addition candidate value j; the security judging device searches for a candidate value h meeting a security condition such as almost prime number characteristic from the class H; and the parameter deciding device computes a parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a, the prime number b, and the prime number p.